УТВЕРЖДАЮ
Директор
ГБУЗВО «Кольчугинская ЦРБ»

_____Матвеева И.В.

«_30_» _марта_ 2017г.

ИНСТРУКЦИЯ
по обеспечению безопасности рабочих мест обработки персональных данных ГБУЗ ВО «Кольчугинская ЦРБ»

2017г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет требования по защите рабочих мест ИСПДн, на которых ведется обработка и хранение персональных данных.

1.2. Настоящая инструкция составлена на основании требований нормативных документов ФСТЭК России.

1.3. В понятие защиты рабочих мест ИСПДн входит:

– физическая защита технических средств от несанкционированного доступа;

– парольная защита рабочих мест от несанкционированного доступа к персональных данным;

– антивирусная защита рабочих мест от несанкционированного доступа к персональным данным из сети Интернет.

2. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В соответствии с требованиями нормативных документов ФСТЭК России методами и способами защиты информации от несанкционированного доступа являются:

2.1. реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

2.2. ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

2.3. разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

2.4. регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

2.5. учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

2.6. резервирование технических средств, дублирование массивов и носителей информации;

2.7. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

2.8. использование защищенных каналов связи;

2.9. размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

2.10. организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

2.11. предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

4. ТРЕБОВАНИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

4.1. На каждом рабочем месте и серверах ИСПДн должно быть установлено антивирусное программное обеспечение (АВПО).

4.2. Антивирусные базы всегда должны быть в актуальном состоянии.

4.3. Запрещается работа на элементах ИСПДн с выключенным или неработоспособным АВПО.

4.4. Определение параметров и режимов работы средств антивирусного контроля осуществляется администратором безопасности (АБ) ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

4.5. Проверка на наличие вирусов должна проводиться регулярно. Проверке подлежат:

- все файлы на жестких дисках серверов и рабочих мест;
- съемные носители, содержащие персональные данные;
- получаемые из сторонних организации файлы;
- передаваемые в сторонние организации файлы.

4.6. Результаты проверок должны фиксироваться в Журнале антивирусных проверок (Приложение 2).

4.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно сообщить о своих подозрениях АБ. АБ совместно с пользователем должен выполнить внеочередной антивирусный контроль.

5. ТРЕБОВАНИЯ ПО РАБОТЕ В СЕТИ ИНТЕРНЕТ

5.1. Работа в сети Интернет на элементах ИСПДн, должна проводиться при служебной необходимости.

5.2. При работе в сети Интернет запрещается:

– Осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран).

– Передавать по сети защищаемую информацию без использования средств шифрования.

– Загружать нелицензионное программное обеспечение.

– Посещать сайты сомнительной репутации (сайты содержащие нелегально распространяемое ПО и т.п.).

6. ТРЕБОВАНИЯ ПО РАБОТЕ СО СРЕДСТВАМИ ЗАЩИТЫ

6.1. На рабочих местах и серверах ИСПДн, исходя из Частной модели актуальных угроз, должны быть установлены специальные средства защиты. К ним относятся:

- средства защиты от несанкционированного доступа;
- межсетевые экраны;
- антивирусные средства защиты.

6.2. Все средства защиты могут быть установлены только организацией, имеющей лицензию на техническую защиту конфиденциальной информации.

6.3. Все средства защиты, установленные в ИСПДн, а также эксплуатационная документация на них, подлежат учету в Журнале учета средств защиты (Приложение 3).

6.4. Настройка средств защиты проводиться в соответствии с эксплуатационной документацией и требованиями нормативных документов ФСТЭК России.

Приложение 1

Форма Журнала учета Логинов

№	Ф И О	Должность	Подразделение	Логин	Дата заведения	Дата удаления	Причина удаления	Подпись системного администратора

Приложение 2

Форма Журнала учета антивирусных проверок

№	Дата проверки	Форма проверки (регулярная/внепланова)	Проверенные АРМ	Результат проверки	Подпись АБ

Приложение 3

Форма Журнала учета СЗИ

№	Уч.№ СЗИ	Наименование СЗИ	Место установки	Дата установки	Подпись установившего	Дата изъятия	Подпись изъявшего